EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	12	human adj interactive adj proofs and captcha	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 15:46
L5	817	(705/64).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/05/24 15:47
L6	2	5 and captcha	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 15:47
L7	6328	(705/1).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/05/24 15:47
L8	1	7 and captcha	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 15:47
L9	7739	((713/182) or (713/168) or (713/170) or (713/176) or (726/26-30)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/05/24 15:50
L10	45	captcha	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 15:51
L11	40	human adj interactive adj proofs	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 15:51
L12	19	reverse adj turing adj test	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 15:51

EAST Search History

L13	7	9 and (L10 L11 L12)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 15:52
L14	1	(trusted black adj box) near3 (located stored resident built adj in local) near4 ((client user) near3 (computer terminal device)) with (generat$3 near3 (nonce challenge))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 15:57
L15	1	(trusted black adj box) near3 (located stored resident built adj in local) near4 ((client user) near3 (computer terminal device node workstation machine)) with (generat$3 near3 (nonce challenge))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 15:57
L16	1	(trusted black adj box) near3 (located stored resident built adj in local) near4 ((client user) near3 (computer terminal device node workstation machine)) with ((creat$3 generat$3) near3 (nonce challenge))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 16:02
L17	1	(trusted black adj box) near3 (located stored resident built adj in local) near4 ((client user) near3 (computer terminal device node workstation machine)) with ((creat$3 generat$3) near3 (random pseudo adj random nonce challenge))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 16:03
L18	3	(secure trusted black adj box) near3 (located stored resident built adj in local) near4 ((client user) near3 (computer terminal device node workstation machine)) with ((creat$3 generat$3) near3 (random pseudo adj random nonce challenge))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 16:03
S1	42	captcha	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 14:26

EAST Search History

S2	9	captcha and signature	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 14:30
S3	40	human adj interactive adj proofs	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 15:43
S4	19	reverse adj turing adj test	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/21 21:39
S5	554	generat$3 with challenge with user	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/21 14:24
S6	49	generat$3 with challenge with user same signature	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/21 14:24
S7	0	("2002/0174348").URPN.	USPAT	OR	ON	2007/05/21 14:38
S8	953	biometric same (hash signature)	USPAT	OR	ON	2007/05/21 14:38
S9	8	evaluat$3 with biometric same (hash signature)	USPAT	OR	ON	2007/05/21 14:39
S10	3	("5677989" | "5764789" | "5815252").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/21 15:10
S11	1	("6,134,340").PN.	US-PGPUB; USPAT	OR	OFF	2007/05/21 15:10
S12	4	("4646352" | "4790564" | "4896363" | "5067162").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/21 15:12
S13	53	("4896363").URPN.	USPAT	OR	ON	2007/05/21 15:15
S14	23	"6,038,666"	USPAT	OR	ON	2007/05/21 15:15
S15	1	("6,038,666").PN.	US-PGPUB; USPAT	OR	OFF	2007/05/21 18:45
S16	20	("6038666").URPN.	USPAT	OR	ON	2007/05/21 16:44

EAST Search History

S17	13	third adj party with generat$3 with challenge	US-PGPUB; USPAT	OR	ON	2007/05/21 21:57
S18	2	challenge same partial adj signature	US-PGPUB; USPAT	OR	ON	2007/05/22 17:35
S19	20	(generate generating) with challenge with user's adj (computing adj device computer terminal)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/21 19:39
S20	249	digital adj signature with challenge	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/21 19:40
S21	1	partial adj digital adj signature with challenge	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/21 19:40
S22	44	third adj party with (issue$2 generat$3) with challenge	US-PGPUB; USPAT	OR	ON	2007/05/22 18:58
S23	9	human adj interactive adj proofs and signature	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/21 21:32
S24	6	reverse adj turing adj test and signature	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/21 21:39
S25	2	"20050120201"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/21 21:42
S26	319	third adj party with challenge	US-PGPUB; USPAT	OR	ON	2007/05/21 21:57
S27	79	third adj party with challenge	USPAT	OR	ON	2007/05/21 21:57

EAST Search History

S28	4	(captcha human adj interactive adj proofs reverse adj turing adj test) and trusted adj third adj party	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 14:01
S29	42	challenge same trusted adj third adj party	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 14:01
S30	1288	third adj party near4 authentication	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 15:14
S31	24	third adj party near4 authentication same challenge	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 14:26
S32	9	human adj interactive adj proofs and signature	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 14:29
S33	6	captcha and hash	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 14:30
S34	12	captcha and encrypt$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 14:31
S35	9	third adj party near4 authentication same digital adj signature with (verify verification)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 15:17

EAST Search History

S36	15	authentication adj authority same digital adj signature with (verify verification)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 15:19
S37	759	authority same digital adj signature with (verify verification)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 15:19
S38	287	authority same digital adj signature with (verify verification) not S36	USPAT	OR	ON	2007/05/22 15:27
S39	94	intermediary with authentication	USPAT	OR	ON	2007/05/22 15:27
S40	6	intermediary with authentication same digital adj signature	USPAT	OR	ON	2007/05/22 15:36
S41	4	radius same digital adj signature	USPAT	OR	ON	2007/05/22 15:36
S42	1	radius adj server same digital adj signature	USPAT	OR	ON	2007/05/22 15:38
S43	2	arbitrated with authentication	USPAT	OR	ON	2007/05/22 15:38
S44	38	arbitrat$3 with authentication	USPAT	OR	ON	2007/05/22 15:38
S45	27	("5586250" | "5623601" | "5708780" | "5778174" | "5933498" | "5944794" | "5950195" | "5987611" | "6058426" | "6061650" | "6092196" | "6119143" | "6122639" | "6163844" | "6167445" | "6167446" | "6198824" | "6219786" | "6226752" | "6233618" | "6292465" | "6310889" | "6317837" | "6317838" | "6321337" | "6345300" | "6351775").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/22 17:17
S46	1	partial adj digital adj signature with challenge	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/22 17:18
S47	23	partial adj digital adj signature	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/22 17:18
S48	514	challenge same digital adj signature	US-PGPUB; USPAT	OR	ON	2007/05/22 17:35
S49	233	challenge with digital adj signature	US-PGPUB; USPAT	OR	ON	2007/05/22 18:53
S50	97	generat$3 adj (challenge nonce) near3 (user client)	US-PGPUB; USPAT	OR	ON	2007/05/22 18:53
S51	6	third adj party near4 (issue$2 generat$3) near5 challenge	US-PGPUB; USPAT	OR	ON	2007/05/22 21:10

EAST Search History

S52	0	challenge with corrupted adj signature	US-PGPUB; USPAT	OR	ON	2007/05/22 20:56
S53	1	challenge with corrupted near3 signature	US-PGPUB; USPAT	OR	ON	2007/05/22 20:56
S54	2	third adj party near4 (issue$2 generat$3) with nonce	US-PGPUB; USPAT	OR	ON	2007/05/22 21:11
S55	2	"20050235342"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/22 22:53
S56	1	("20050166052").PN.	US-PGPUB; USPAT	OR	OFF	2007/05/22 22:53

Term used **captcha** Found **54** of **201,798**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 54 Result page: **1** 2 3 next

Relevance scale

1 Poster 2: applications track: IMAGINATION: a robust image-based CAPTCHA generation system

Ritendra Datta, Jia Li, James Z. Wang
November 2005 **Proceedings of the 13th annual ACM international conference on Multimedia MULTIMEDIA '05**
Publisher: ACM Press
Full text available: pdf(308.63 KB) Additional Information: full citation, abstract, references, index terms

We propose IMAGINATION (IMAge Generation for INternet AuthenticaTION), a system for the generation of attack-resistant, user-friendly, image-based CAPTCHAs. In our system, we produce controlled distortions on randomly chosen images and present them to the user for annotation from a given list of words. The distortions are performed in a way that satisfies the incongruous requirements of low perceptual degradation and high resistance to attack by content-based image retrieval systems. Word choice ...

Keywords: CAPTCHA, automated turing test, image retrieval

2 Keeping bots out of online games

Philippe Golle, Nicolas Ducheneaut
June 2005 **Proceedings of the 2005 ACM SIGCHI International Conference on Advances in computer entertainment technology ACE '05**
Publisher: ACM Press
Full text available: pdf(133.20 KB) Additional Information: full citation, abstract, references

We study the problem of restricting participation in online games to human players, so they can enjoy the game without interference from automated playing agents known as bots. We propose a range of techniques, both software and hardware based, to distinguish bots from human players in a wide variety of online games, from poker to "shoot'em ups."

3 Games: Preventing bots from playing online games

Philippe Golle, Nicolas Ducheneaut
July 2005 **Computers in Entertainment (CIE)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(210.16 KB) Additional Information: full citation, abstract, references, index terms

As multiplayer online gaming gains in economic and social importance, an increasingly

large number of players is beginning to rely on bots (automated player agents) to gain unfair advantages in games. In this article we study the problem of restricting participation in online games to human players so they can enjoy the game without interference from the bots. We propose two broad approaches to prevent bots from playing online games. The first consists of seamlessly integrating software-based te ...

Keywords: CAPTCHAs, agents, bots, games, reverse Turing test

4 Telling humans and computers apart automatically

Luis von Ahn, Manuel Blum, John Langford
February 2004 **Communications of the ACM**, Volume 47 Issue 2
Publisher: ACM Press
Full text available: pdf(106.33 KB) html(18.53 KB) Additional Information: full citation, abstract, references, citings, index terms

How lazy cryptographers do AI.

5 Towards Blocking Outgoing Malicious Impostor Emails

Erhan J. Kartaltepe, Shouhuai Xu
June 2006 **Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks WOWMOM '06**
Publisher: IEEE Computer Society
Full text available: pdf(320.41 KB) Additional Information: full citation, abstract, index terms

Electronic mails (emails) have become an indispensable part of most people's daily routines. However, they were not designed for deployment in an adversarial environment, which explains why there have been so many incidents such as spamming and phishing. Malicious impostor emails sent by sophisticated attackers are perhaps even more damaging, because their contents, except the attachments, may look perfectly legitimate while silently targeting certain critical information such as cryptographic k ...

6 Communication privacy: How to achieve blocking resistance for existing systems enabling anonymous web surfing

Stefan Köpsell, Ulf Hillig
October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic society WPES '04**
Publisher: ACM Press
Full text available: pdf(897.66 KB) Additional Information: full citation, abstract, references, index terms

We are developing a blocking resistant, practical and usable system for anonymous web surfing. This means, the system tries to provide as much reachability and availability as possible, even to users in countries where the free flow of information is legally, organizationally and physically restricted. The proposed solution is an add-on to existing anonymity systems. First we give a classification of blocking criteria and some general countermeasures. Using these techniques, we outline a conc ...

Keywords: AN.ON, JAP, Mix, blocking resistance

7 Multi-agent systems and social behavior: Blind sales in electronic commerce

E. Aïmeur, G. Brassard, F. S. Mani Onana
March 2004 **Proceedings of the 6th international conference on Electronic commerce ICEC '04**
Publisher: ACM Press
Full text available: pdf(330.05 KB) Additional Information: full citation, abstract, references, citings

We start with the usual paradigm in electronic commerce: a consumer who wants to buy from a merchant. However, both parties wish to enjoy maximal privacy. In addition to remaining anonymous, the consumer wants to hide her browsing pattern and even the identification of the product she may decide to buy. Nevertheless, she wants to be able to negotiate the price, pay, receive the product and even enjoy maintenance on it. On the other hand, the merchant wants to leak as little information as possib ...

Keywords: CAPTCHA, anonymous surfing, cryptography, customer buying behaviour, electronic commerce, oblivious transfer, private information retrieval

8 Session 1: On instant messaging worms, analysis and countermeasures

Mohammad Mannan, Paul C. van Oorschot
November 2005 **Proceedings of the 2005 ACM workshop on Rapid malcode WORM '05**
Publisher: ACM Press

Full text available: pdf(186.53 KB) Additional Information: full citation, abstract, references, citings, index terms

We provide a collection of minor results on the area of Instant Messaging (IM) worms, which has received relatively little attention in the formal literature. We review selected IM worms and summarize their main characteristics, motivating a brief overview of the network formed by IM contact lists, and a discussion of theoretical consequences of worms in such networks. Existing methods to restrict an IM worm epidemic are analyzed in terms of usability and effectiveness, leading to the suggestion ...

Keywords: instant messaging worms, scale-free networks

9 DDoS defense by offense

Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger, Scott Shenker
August 2006 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '06**, Volume 36 Issue 4
Publisher: ACM Press
Full text available: pdf(334.96 KB) Additional Information: full citation, abstract, references, index terms

This paper presents the design, implementation, analysis, and experimental evaluation of *speak-up*, a defense against *application-level* distributed denial-of-service (DDoS), in which attackers cripple a server by sending legitimate-looking requests that consume computational resources (*e.g.*, CPU cycles, disk). With speak-up, a victimized server encourages all clients, resources permitting, *to automatically send higher volumes of traffic*. We suppose that attackers are a ...

Keywords: DoS attack, bandwidth, currency

10 Secure distributed human computation

Craig Gentry, Zulfikar Ramzan, Stuart Stubblebine
June 2005 **Proceedings of the 6th ACM conference on Electronic commerce EC '05**
Publisher: ACM Press
Full text available: pdf(257.80 KB) Additional Information: full citation, abstract, references, index terms

This paper is a preliminary exploration of secure distributed *human* computation. We consider the general paradigm of using large-scale distributed computation to solve difficult problems, but where humans can act as agents and provide candidate solutions. We are especially motivated by problem classes that appear to be difficult for computers to solve effectively, but are easier for humans; e.g., image analysis, speech recognition,

and natural language processing. This paradigm already se ...

Keywords: B24b, human distributed computation

11 DOS protection: Using graphic turing tests to counter automated DDoS attacks against web servers

William G. Morein, Angelos Stavrou, Debra L. Cook, Angelos D. Keromytis, Vishal Misra, Dan Rubenstein

October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**

Publisher: ACM Press

Full text available: pdf(256.83 KB) Additional Information: full citation, abstract, references, citings, index terms

We present WebSOS, a novel overlay-based architecture that provides guaranteed access to a web server that is targeted by a denial of service (DoS) attack. Our approach exploits two key characteristics of the web environment: its design around a human-centric interface, and the extensibility inherent in many browsers through downloadable "applets." We guarantee access to a web server for a large number of *previously unknown* users, without requiring pre-existing trust relationships between ...

Keywords: Java, graphic turing tests, web proxies

12 Authentication and authorization: Securing passwords against dictionary attacks

Benny Pinkas, Tomas Sander

November 2002 **Proceedings of the 9th ACM conference on Computer and communications security CCS '02**

Publisher: ACM Press

Full text available: pdf(216.72 KB) Additional Information: full citation, abstract, references, citings, index terms

The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by automated programs running dictionary attacks. Passwords remain the most widely used authentication method despite their well-known security weaknesses. User authentication is clearly a practical problem. From the perspective of a service provider this problem needs to be solved within real-world constraints such as the available hardware and software infrastructures. From a user' ...

13 Scalability in MMOGs: Towards public server MMOs

Chris Chambers, Wu-chang Feng, Wu-chi Feng

October 2006 **Proceedings of 5th ACM SIGCOMM workshop on Network and system support for games NetGames '06**

Publisher: ACM Press

Full text available: pdf(190.33 KB) Additional Information: full citation, abstract, references, index terms

While massively multiplayer on-line games (MMOs) are enormously popular, their use of the client-server architecture causes them to suffer from scalability issues and high maintenance costs. In contrast, the public server architecture employed by most first-person shooter (FPS) games scales more easily by relying on user-supplied hosting and user-generated content, but lacks persistence between servers that is required in the MMO genre. This paper examines an architecture that leverages the r ...

Keywords: MMO, online games

14 Reception and posters: ARTiFACIAL: automated reverse turing test using FACIAL features

Yong Rui, Zicheg Liu
November 2003 **Proceedings of the eleventh ACM international conference on Multimedia MULTIMEDIA '03**
Publisher: ACM Press

Full text available: pdf(360.48 KB) Additional Information: full citation, abstract, references, citings, index terms

Web services designed for human users are being abused by computer programs (bots). The bots steal thousands of free email accounts in a minute; participate in online polls to skew results; and irritate people by joining online chat rooms. These real-world issues have recently generated a new research area called Human Interactive Proofs (HIP), whose goal is to defend services from malicious attacks by differentiating bots from human users. In this paper, we propose a new HIP algorithm based on ...

Keywords: CAPTCHA, face and facial feature detection, human interactive proof (HIP), turing test, web services security

15 Demonstration session 2: Excuse me, but are you human?

Yong Rui, Zicheg Liu
November 2003 **Proceedings of the eleventh ACM international conference on Multimedia MULTIMEDIA '03**
Publisher: ACM Press

Full text available: pdf(175.38 KB) Additional Information: full citation, abstract, references, index terms

Web services designed for human users are being abused by computer programs (bots). The bots steal thousands of free email accounts in a minute; participate in online polls to skew results; and irritate people by joining online chat rooms. These real-world issues have recently generated a new research area called Human Interactive Proofs (HIP), whose goal is to defend services from malicious attacks by differentiating bots from human users. We propose a new HIP algorithm based on detecting human ...

Keywords: CAPTCHA, face and facial feature detection, human interactive proof (HIP), turing test, web services security

16 Email and security: Designing human friendly human interaction proofs (HIPs)

Kumar Chellapilla, Kevin Larson, Patrice Simard, Mary Czerwinski
April 2005 **Proceedings of the SIGCHI conference on Human factors in computing systems CHI '05**
Publisher: ACM Press

Full text available: pdf(471.32 KB) Additional Information: full citation, abstract, references, index terms

HIPs, or Human Interactive Proofs, are challenges meant to be easily solved by humans, while remaining too hard to be economically solved by computers. HIPs are increasingly used to protect services against automatic script attacks. To be effective, a HIP must be difficult enough to discourage script attacks by raising the computation and/or development cost of breaking the HIP to an unprofitable level. At the same time, the HIP must be easy enough to solve in order to not discourage humans from ...

Keywords: completely automated public turing tests to tell computers and humans apart (CAPTCHAs), computer vision, evaluation, human interaction proofs (HIPs), human perception, visual letter recognition

17 Q focus: cybercrime: Criminal code: the making of a cybercriminal

Thomas Wadlow, Vlad Gorelik
November 2006 **Queue**, Volume 4 Issue 9
Publisher: ACM Press
Full text available: pdf(1.13 MB) htm(23.18 KB) Additional Information: full citation, abstract, index terms

Queue's first-ever narrative chronicles one man's transition from small-time hacker to big-time crook.

18 AI update: AI update

D. R. Hobaugh
December 2001 **intelligence**, Volume 12 Issue 4
Publisher: ACM Press
Full text available: pdf(356.69 KB) html(36.90 KB) Additional Information: full citation, index terms

19 Fighting the spam wars: A remailer approach with restrictive aliasing

Pawel Gburzynski, Jacek Maitan
February 2004 **ACM Transactions on Internet Technology (TOIT)**, Volume 4 Issue 1
Publisher: ACM Press
Full text available: pdf(162.34 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We present an effective method of eliminating unsolicited electronic mail (so-called *spam*) and discuss its publicly accessible prototype implementation. A subscriber to our system is able to obtain an unlimited number of aliases of his/her permanent (protected) E-Mail address to be handed out to parties willing to communicate with the subscriber. It is also possible to set up publishable aliases, which can be used by human correspondents to contact the subscriber, while being useless to h ...

Keywords: Electronic mail, privacy, spam

20 A new privacy model for hiding group interests while accessing the Web

Yuval Elovici, Bracha Shapira, Adlai Maschiach
November 2002 **Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society WPES '02**
Publisher: ACM Press
Full text available: pdf(104.19 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a new privacy model for hiding the information interests of a homogenous group of users who share a local area network and an access point to the Web. The suggested model is aimed at preventing eavesdroppers from using identifiable members' tracks to infer the group common interests (referred to as the group profile) while allowing members of the group to identify themselves to various services. The model consists of generating faked transactions in various fields of interest ...

Keywords: Web-security, privacy, user-groups, user-profile